

REMARKS

This amendment is in response to the Official Action dated July 9, 2008. Claim 20 has been amended to fix a typographical error only, claims 9 and 12 have been canceled; as such claims 1-4, and 14-24 are now pending in this application. Claims 1-4, 14, 18, 20, and 22 are independent claims. Reconsideration and allowance is requested in view of the claim amendments and the following remarks.

No new matter has been added by this Amendment.

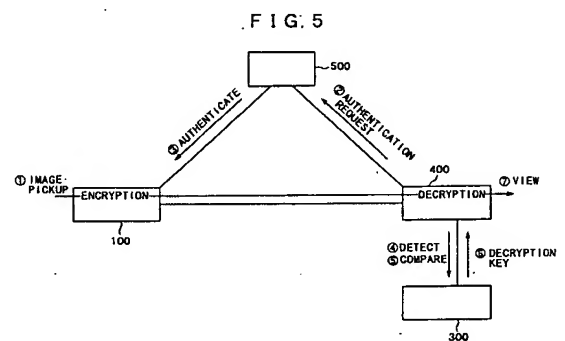
An Example Embodiment

FIG. 5 illustrates an example embodiment of the present invention having an image pickup device 100, authentication server 500, Viewer 400, and decryption key storage device 500. A viewer 400 can communicate directly with image pickup device 100, after authentication by authentication server 500. A viewer 400 seeking to communicate with image pickup device 100 will contact authentication server 500 with security information, such as a serial number for the image pickup device.

The disclosed system includes two points of security to protect the viewing of images from the image pickup 100:

First, communications between a viewer and an image pickup must be authorized by the authentication server 500. A designated viewer 400 can only communicate with a given image pickup device 100.

Second, the encryption/decryption keys at the given image pickup device 100 and the designated viewer 400 must match. This ensures that no entity between the image pickup device 100 and the designated viewer 400 can intercept and decrypt an encrypted image from the image pickup device 100.



Rejections under 35 U.S.C. § 102

Claims 9 and 12 are rejected under 35 USC § 102 as anticipated by U.S. Patent Pub. No. 2002/0118837 to Hamilton.

This rejection is moot due to the cancellation of claims 9 and 12.

Rejections under 35 U.S.C. § 103

Claims 1-4 have been rejected under 35 U.S.C. § 103 over U.S. Patent Pub. No. 2004/0066456 to Read in view of Hamilton. Claims 14-17 and 22-24 have been rejected under 35 U.S.C. § 103 over Hamilton in view of Read. This rejection is traversed.

Claim 1 recites: *An image transmission system for transmitting an image via a network, said image transmission system comprising:*

one or a plurality of image pickup apparatus each having a unique identifying number and having an encrypting function for encrypting a picked-up image for transmission to said network;

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image;

a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other;

a viewing apparatus connected to said removable recording medium, having a decrypting function for decrypting said encrypted image using said decryption key, for communicating with said image pickup device, and for viewing the image transmitted via said network from said image pickup apparatus to the viewing apparatus; and

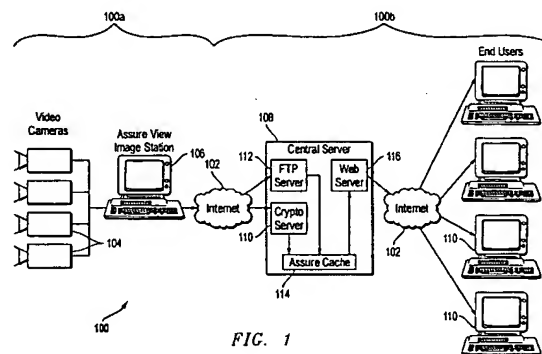
an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.

With respect to claim 1, neither Read nor Hamilton disclose “*a viewing apparatus ... having a decrypting function for decrypting said encrypted image using said decryption key... and an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.*”

Claim 1 recites “a viewing apparatus ... having a decrypting function for decrypting said encrypted image using said decryption key.” The *encrypted image* is created by “one or a plurality of image pickup apparatus each having a unique identifying number and having an encrypting function for encrypting a picked-up image.” The significance of transferring the image in its encrypted format ensures the viewing party that the image has not, and cannot be viewed by intermediate parties.

Furthermore, claim 1 discloses “an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.” Paragraph [0115] of the specification discusses the authentication process as dealing with ensuring that a given viewing apparatus may access a given imaging pick-up device. Furthermore, the line of the claim sets forth two requirements: (1) that the “*authenticating server [] authenticat[e] said image pickup apparatus*” and (2) that the “*image pickup apparatus [be] accessible from said viewing apparatus.*”

Read discloses a central server 108 that retrieves, decrypts, and stores encrypted images from the imaging device 104 and image station 106. These decrypted images can then be viewed by End Users 110 that have access to central server 108. No communication passes *unmodified* between the End User 110 and the Imaging device, or vice versa.



Unlike the claimed invention, the End Users 110 do not decrypt the image from the video cameras 104. That is, the end users 110 do not “*hav[e] a decrypting function for decrypting [] encrypted image using [a] decryption key.*”

Furthermore, even if the end user 110 did use a decryption function, they would not receive the “encrypted image” which was encrypted by the image pickup device. By distinction, in defining the “encrypted image” the claim recites “one or a plurality of image pickup apparatus each ... having an encrypting function for encrypting a picked-up image.” This identifies the encrypted image as being an encrypted image from the image pick-up apparatus in the encrypted format.

As explained above, the significance of transferring the image in its encrypted format ensures the viewing party that the image has not, and cannot be viewed by intermediate parties. This distinguished the claim from Read because, in Read, the decrypted images are stored at the central server and can be viewed by anyone who obtains access to the central server. Read fails to send any encrypted image form the video cameras 104 to the end users 110 in the encrypted format.

Also unlike the claimed invention, Read does not employ “an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.” The specification discusses the authentication process with respect to ensuring that a given viewing apparatus may access a given imaging pick-up device. This line of the claim sets forth two requirements: (1) that the “authenticating server [] authenticat[e] said image pickup apparatus” and (2) that the “image pickup apparatus [be] accessible from said viewing apparatus.”

First, Read does not *authenticate* a given image apparatus as disclosed in the claims. The central server does not authenticate, and thereby authorize, communication between the image pickup device and the viewer. Instead, the central server 108 decrypts images from the video cameras and stores those images. Thereafter, the central server controls access to those decrypted images, not to the video cameras.

Second, accessing an imaging apparatus from a viewing apparatus, is not considered within the architecture of the Read system. As such, Read does not disclose that the “image pickup apparatus [is] accessible from said viewing apparatus.”

Hamilton is directed to systems where the authentication of an image is critical, e.g., in cases of insurance investigations and court photographs. The problem being remedied is that digital images are easily modified, therefore a method for ensuring the authenticity of a given digital image becomes critical.

The system operates by providing one set of

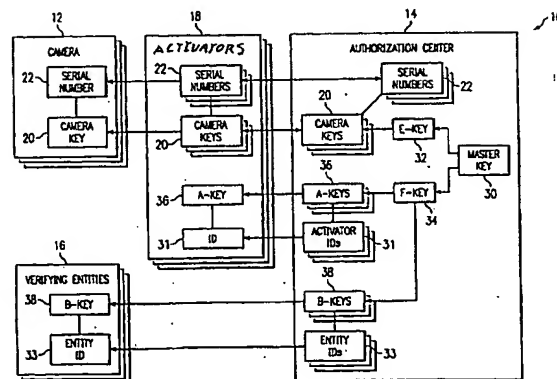


FIG. 2

encryption keys (A-keys) to cameras 12, and a different set of encryption keys (B-keys) to viewing devices (verifying entities 16). *The A-keys are unrelated to B-keys.* That is, A-key encrypted images cannot be decrypted using B-keys, or vice versa.

The mechanism ensures an image's authenticity from each camera using A-key encryption to send images taken by the cameras to the central server 14. That is, Secure communication between the central server 14 and cameras 12 *are encrypted using A-keys.* To ensure an image's authenticity an image viewed at the verifying entity 16 can only be verified against an image in the authentication center 14. Secure communication between the central server and verifying entities *are encrypted using B-keys.*

As such, no secure communication can take place between the cameras and the verifying entities using the same encryption keys. Communication can *only* take place between the central server 14 and cameras 12 using A-keys to transfer images, and between the central server 14 and verifying entities are encrypted using B-keys to verify images. As such, the Read system also lacks the security feature recited in claim 1.

As disclosed above, claim 1 recites viewers that “*hav[e] a decrypting function for decrypting [] encrypted image using [a] decryption key.*” The *encrypted image* disclosed in the claim corresponds to the encrypted image *encrypted by* the image pick-up device.

However, in Hamilton, the image from the viewer that is compared at the Authorization Center 14 is encrypted using a different encryption key than that used by the camera 12. Again, the significance of transferring the image in its encrypted format ensures the viewing party that the image has not, and cannot be viewed by intermediate parties *such as a central server.* This is exactly the opposite of Hamilton, where the Authorization Center 14 decrypts and stores a copy of the image from camera 12.

Furthermore, Hamilton fails to disclose “*an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus,*” because Hamilton intentionally prevents the viewing apparatus from having direct access to the camera 12. Instead, Hamilton treats the communication between the central server 14 and camera 12, and communication between the central server 14 and entity 18 as distinct as is evident by the use of different encryptions keys for each type of communication.

Even if Hamilton and Read were combinable (which is not admitted), Applicant submits that the combination would fail to teach or suggest “*a viewing apparatus ... having a decrypting function for decrypting said encrypted image using said decryption key... and an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.*” This is because neither reference address the form of secure communication claimed. That is, neither reference seeks to ensure encrypted communication between a viewer and a camera, such that no intervening entity can view the images. Furthermore, neither employs an authorization scheme for communications between a camera and viewer and claimed.

Therefore, because even a combination of the relied upon references would still fail to yield the claimed invention, Applicant submits that a *prima facie* case of obviousness for claim 1 has not been presented. For the reasons stated above, claims 2-4, 14-17, and 22-24 also overcome Hamilton and Read.

Accordingly, Applicant respectfully requests that the rejection of independent claims 1-4 and under 35 U.S.C. § 103(a) be withdrawn.

Claims 18-21 have been rejected under 35 U.S.C. §103 over U.S. Patent Pub. No. 2004/0085446 to Park, in view of Read in view of U.S. Patent No. 6,999,588 to Oishi.

Amended claim 18 recite: *A computer program, stored on a computer readable medium, for making a computer perform comprising the steps of: ...*

requesting that the authentication server authenticate a user and authenticate that a user can access the image pickup device;

authenticating the user and image pickup apparatus in response to the requesting step;

connecting the image pickup apparatus to a viewing apparatus;

comparing the identification number in the memory card to the identifying number of the image pickup apparatus;

obtaining the decryption key from the memory card;

transmitting an image request from the viewing apparatus to the image pickup apparatus;

receiving an image from the imaging pickup apparatus at the viewing apparatus;

decrypting images received from the image pickup device using the decryption key;

displaying the decrypted images on the viewer.

With respect to claim 18, neither Park, Hamilton, nor Oishi teach or suggest the authentication steps of “*requesting that the authentication server authenticate a user and authenticate that a user can access the image pickup device; authenticating the user and image pickup apparatus in response to the requesting step,*” and then the direct communication steps of “*transmitting an image request from the viewing apparatus to the image pickup apparatus.*”

Park describes a security system that allows remote monitoring of video cameras, but lacks the ability to use a common server to authenticate viewers, as being authorized to receive video or images from a given camera. While Park disclose using encrypted communications between a camera 100 and PC 300, Park does not employ an authorization component because the PC 300 and Camera 100 are intended to function using a serial data connection; that is, the camera is intended to be in the immediate vicinity of the PC, not in a remote location.

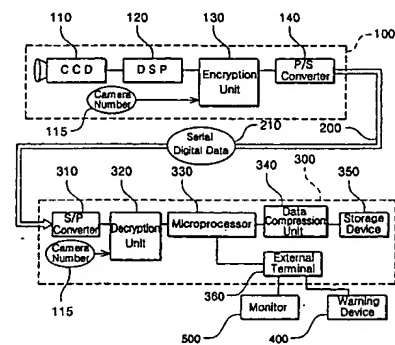


Fig. 2

Hamilton simply discloses a method of authenticating images at a central authentication server, which simply acts as an image repository for comparing an incoming image from a user with another image in the repository.

Finally, Oishi teaches a method by which images can be encrypted using an IC card.

However, all these references fail to teach or suggest the concept of initially passing communications through an authentication server to verify a viewer before allowing communication directly between the viewer and the imaging apparatus. That is, none of the references allow both the use of an authentication server to begin communication and direct communication between the imaging device and the viewer thereafter. There is simply no motivation in any of the references to this two-part communication scheme involving both server authorization and encryption.

Even if Park, Read, and Oishi were combinable (which is not admitted), Applicant submits that the combination would fail to teach or suggest “*authenticating the user and image pickup apparatus in response to the requesting step; connecting the image pickup apparatus to a viewing apparatus,*” and “*transmitting an image request from the viewing apparatus to the image pickup apparatus; receiving an image from the imaging pickup apparatus at the viewing apparatus.*”

Instead, a combination of Park, Read, and Oishi would necessarily yield a video camera system as in Park, but would pass all communication through a central server for image decryption and storage, as in Read, and would use the authentication mechanism, as in Oishi.

Since even a combination of the relied upon references would still fail to yield the claimed invention, Applicant submits that a prima facie case of obviousness for claim 18 has not been presented. Applicant also notes that the offered combination appears to be a (failed) attempt to reconstruct the claimed invention in hindsight, as there is no basis to combine Park, Read, and Oishi to produce the claimed invention.

For similar reasons, claim 20 also overcomes the combination of Park, Read, and Oishi. For the reasons stated above, claims 19 and 21 also overcome the combination of Park, Read, and Oishi because they depend on independent claims 18 and 20.

Accordingly, Applicant respectfully requests that the rejection of independent claim 18 and dependent claims 19-21 under 35 U.S.C. § 103(a) be withdrawn.

In view of the above amendment, applicant believes the pending application is in condition for allowance.

CONCLUSION

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-2960 from which the undersigned is authorized to draw.

Dated: September 16, 2008

Respectfully submitted,

By  4/29/08

Ronald P. Kananen

Registration No.: 24,104

Christopher M. Tobin

Registration No.: 40,290

Ronald P. Kananen

Registration No.: 24,104

RADER, FISHMAN & GRAUER PLLC

Correspondence Customer Number: 23353

Attorneys for Applicant